



an unsecured side of a firewall, the firewall having a secured side and the unsecured side;

at least one secure communication link between the plurality of host machines;

5 a filing storage system accessible by at least one of the plurality of host machines, the filing storage system having a storeroom area and a customer account area, wherein the filing storage system supports hard file links between the storeroom area and the customer account area, the hard file links comprising pointers to files [with a hard linking capability there between];

10 [a firewall with] at least one secured host machine residing on the secured side of the firewall; and

15 a customer account database located on the secured host machine and accessible by at least one of the plurality of host machines across a second secure[d] communication link through the firewall.

A
2. (Once amended) The [apparatus] system of Claim 1, wherein the at least one secure communication link utilizes a protocol for the exchange of arbitrary sized packets of ascii data, delimited by carriage return and newline boundary markers.

25 3. (Once amended) The [apparatus] system of Claim 2, wherein at least one secure communication link [enhances the protocol by utilizing] utilizes DES encryption [with N DES keys, and a method for securely passing the DES keys comprising the steps of:

(i) finding the port number P used for the connection;

30 (ii) computing a value $I = P \text{ modulo } N$; and

(iii) using I as the index into the N keys, and using the DES key residing at index I to encrypt and decrypt the data stream].

6. (Once amended) The [apparatus] system of Claim 1, wherein the [secured] second secure communication link through the firewall utilizes tobj protocol.

7. (Once amended) The [apparatus] system of Claim 1, wherein at least one of the plurality of host machines runs a web server process and at least one separate one of the plurality of host machines runs an ftp server process, whereby a customer web browser contacts the host machines.

8. (Once amended) A method of facilitating the [high speed] transfer of data to authorized users over the [i]Internet, the method comprising [the steps of]:

(i) running a web server process on at least one host machine;

(ii) running an ftp server process on a separate host machine;

(iii) establishing a secure communication link between the host machines;

(iv) establishing [a] at least one hard link between storeroom file storage areas and customer account file storage areas, the at least one hard link comprising a pointer to a file; and

(v) dynamically allocating customer access information from a secured database.

9. (Once amended) The method of Claim 8, wherein [step (iii)] the establishing a secure communication link comprises using [uses] a protocol for the exchange of arbitrary sized packets of ascii data delimited by carriage return and newline boundary markers, and using DES encryption with N keys, step (iii) including the following steps:

(a) finding the port number P used for the connection;

(b) computing an index value I, where $I = P \text{ modulo } N$;

and

(c) using the DES key residing at index I to encrypt and decrypt the data stream.

10. (Once amended) The method of Claim 9, wherein the DES encryption creates a cypher string, further comprising
5 filtering the cypher string [and filtering is applied to render the cypher string at least 7-bit safe].

505B1
11. (Once amended) A[n] system [apparatus] for facilitating the [high speed] transfer of data to authorized users over the [i]Internet, the system [apparatus] comprising:

10 a plurality of host machine means for running a plurality of processes;

A
at least one secure means for communicating between the host machines;

15 [a] file storage means having a storeroom area and a customer account area with a means for securely hard linking between the areas, the hard linking comprising pointers to files;

20 [a] firewall means for providing security between machines, with at least one secured host machine means residing on the secured side of the firewall;

[a] means for databasing customer accounts located on the secured host machine means and accessible by a secured means for communicating through the firewall.

12. The method of claim 8, further comprising issuing at
25 least one change root command to limit access by the authorized users in the customer account file storage areas.

A³
13. The method of claim 8, wherein the establishing at least one hard link between storeroom file storage areas and customer account file storage areas comprises creating a file
30 pointer in the customer account file storage areas which points to a file in the storeroom file storage areas so that

the file in the storeroom file storage areas can be accessed from the customer account file storage areas without copying the file to the customer account file storage areas.

5 14. The method of claim 8, further comprising said web server process receiving a request from one of said authorized users for at least one file.

10 15. The method of claim 14, further comprising said web server process determining whether to provide said at least one file by accessing a database on a host machine through a firewall.

16. The method of claim 8, further comprising said ftp server process allocating space on said customer account file storage areas for said at least one file.

15 17. The method of claim 16, further comprising creating a hard link on said space on said customer account file storage areas, said hard link pointing to said at least one file, wherein said at least one file resides in said storeroom file storage areas.

20 18. The method of claim 16, further comprising allowing at least one of said authorized users to access said space on said customer account file storage areas.

25 19. The method of claim 18, wherein the allowing at least one of said authorized users to access said space on said customer account file storage areas comprises issuing a change root command making said space a root directory for said at least one of said authorized users.
